

AD-A058 801

CORNELL UNIV ITHACA N Y DEPT OF COMPUTER SCIENCE
A NOTE ON CRYPTOGRAPHY AND NPNCONP-P, (U)
APR 78 G BRASSARD, S FORTUNE, J HOPCROFT
CU-CSD-TR-338

F/G 9/4

N00014-76-C-0018

UNCLASSIFIED

NL

OF
AD
A058801



END
DATE
FILMED

11-78
DDC

LEVEL

(12)

AD A058801

DDC FILE COPY

(6) A NOTE ON CRYPTOGRAPHY
AND NPnCoNP-P,

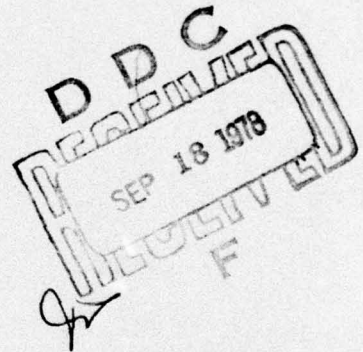
by

(10) Gilles/Brassard,
Steve/Fortune
John/Hopcroft

(14) CU-CSD-TR-338

(11) Apr 78

(12) 8 p.



(15) N00014-76-C-0018

Department of Computer Science
Cornell University
Ithaca, New York 14853

This document has been released
for public release and sale; its
distribution is unlimited.

78 09 05 097 407 072 mt

A NOTE ON CRYPTOGRAPHY
AND $NP \neq CoNP - P$

by

Gilles Brassard
Steve Fortune
John Hopcroft

Department of Computer Science
Cornell University
Ithaca, New York 14853

Abstract

Diffie and Hellman [2] propose [→] the use of the exponential ^{is studied} function in a finite field for cryptographic purposes. The proposal is based on the conjecture that the inverse function, the logarithm, is not feasibly computable. ~~We show that a~~ proof of this conjecture would have important consequences for theoretical computer science, even under the assumption that $P \neq NP$. [←]

does not equal

† This research was supported in part by Office of Naval Research under grant number ONR N00014-76-C-0018.

78 09 05 097

Diffie and Hellman [2] propose the use of the exponential function in a finite field for cryptographic purposes. The proposal is based on the conjecture that the inverse function, the logarithm, is not feasibly computable. We show that a proof of this conjecture would have important consequences for theoretical computer science, even under the assumption that $P \neq NP$.

Our observation is based on the following idea. ($|i|$ here represents the length of binary representation of i).

Proposition:

Suppose f has the following properties: $|f(i)| = |i|$, f is one-one and onto, f is computable in polynomial time and f^{-1} is not polynomial time computable. Then the set $S = \{ \langle n, m \rangle \mid f^{-1}(n) > m \}$ is in $NP \cap CoNP - P$. Moreover, if f^{-1} is NP-hard then $NP = CoNP$.

Proof:

S is in NP, since on input $\langle n, m \rangle$ a nondeterministic algorithm can guess i of length $|n|$, verify $f(i)=n$ and accept if $i > m$. Similarly S is in CoNP (guess i , verify $f(i)=n$ and accept if $i \leq m$). S is not in P, otherwise $f^{-1}(n)$ can be computed in polynomial time as follows. $f^{-1}(n)$ is one of at most $2^{|n|}$ possible values. By binary search where each query $\langle n, k \rangle$ of S divides the range in half, we can uniquely determine $f^{-1}(n)$ within $|n|$ queries. Moreover, if f^{-1} is NP-hard so is S . But $S \in NP \cap CoNP$. Therefore $NP = CoNP$. \square

The function proposed by Diffie and Hellman, namely $\exp_{r,p}(n) \equiv r^n \pmod{p}$, does not quite satisfy the proposition,

ACCESSION for	
NTIS	White S
DDC	Buff Sec
UNANNOUNCED	
JUSTIFICATION	
BY	
DISTRIBUTION/AVAILABILITY CODE	
Dist.	SP. CL.
A	

since it is not length preserving and moreover if p is not prime or r is not a primitive element modulo p , it is not one-one. However, a slightly more complicated proof will obtain a similar result.

Define the logarithm function $\log(p,r,n)$ as follows. If p is a prime and r is a primitive element modulo p , then $\log(p,r,n)$ is the unique m such that $0 < m < p$ and $r^m \equiv n \pmod{p}$. Otherwise $\log(p,r,n)$ is 0.

Theorem:

If $\log(p,r,n)$ is not computable in polynomial time, then $P \not\subseteq NP \cap CoNP$.

Proof:

Consider the set $S = \{(p,r,n,t) \mid \log(p,r,n) > t\}$.

We show S is in NP as follows. p is a prime and r is a primitive element modulo p if and only if $r^{p-1} \equiv 1 \pmod{p}$ and for each q a prime factor of $p-1$, $r^{(p-1)/q} \not\equiv 1 \pmod{p}$ [3]. These conditions can be checked in nondeterministic polynomial time by guessing the prime decomposition of $p-1$ together with certificates [4] that each of the factors is indeed prime. Once it is known that p is prime and r a primitive element, the unique m such that $r^m \equiv n \pmod{p}$ can be guessed. If $m > t$, (p,r,n,t) is in S .

S is also in CoNP. A quadruple (p,r,n,t) is not in S if and only if $\log(p,r,n) \leq t$. The condition is true if and only if either there are i and j , $0 < i < j < p$, such that $r^i \equiv r^j \pmod{p}$ or there is an m such that $r^m \equiv n \pmod{p}$ and $m \leq t$. Both of these conditions can be checked nondeterministically in polynomial time.

Now if we are given an oracle for the set S , $\log(p,r,n)$ can be computed in deterministic polynomial using binary search. Hence if $\log(p,r,n)$ is not polynomial time computable, then S is not in P . \square

Additional material will appear in [1], together with a similar result for the cryptographic method based on prime decomposition suggested in [5].

References

- [1] Brassard, G. "Cryptography and NP \cap CoNP", in preparation, Department of Computer Science, Cornell University (1978).
- [2] Diffie, W. and M.E. Hellman. "New Directions in Cryptography", IEEE Transactions on Information Theory, Volume 22 (1976), pp. 644-654.
- [3] Knuth, D. The Art of Computer Programming, Volume 2: Seminumerical Algorithms, (1969), Addison-Wesley, Reading, MA, page 348.
- [4] Pratt, V. "Every Prime has a Succinct Certificate", Siam Journal on Computing, Volume 4, (1975), pp. 214-220.
- [5] Rivest, R., A. Shamir and L. Adleman. "On Digital Signatures and Public-Key Cryptosystems", MIT Laboratory for Computer Science, Cambridge, Mass., (1977).

Security Classification		DOCUMENT CONTROL DATA - R & D	
<i>(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)</i>			
1. ORIGINATING ACTIVITY (Corporate author) Computer Science Department Cornell University Ithaca, NY 14853		2a. REPORT SECURITY CLASSIFICATION	
		2b. GROUP	
3. REPORT TITLE A Note on Cryptography and NP _n CoNP-P			
4. DESCRIPTIVE NOTES (Type of report and inclusive dates) technical			
5. AUTHOR(S) (First name, middle initial, last name) Giles Brassard, Steve Fortune, John Hopcroft			
6. REPORT DATE April 1978	7a. TOTAL NO. OF PAGES 6	7b. NO. OF REFS 5	
8a. CONTRACT OR GRANT NO. ONR N00014-76-C-0018	8a. ORIGINATOR'S REPORT NUMBER(S) none		
8b. PROJECT NO.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)		
10. DISTRIBUTION STATEMENT Distribution of manuscript is unlimited			
11. SUPPLEMENTARY NOTES		12. SPONSORING MILITARY ACTIVITY	
13. ABSTRACT Diffie and Hellman [2] propose the use of the exponential function in a finite field for cryptographic purposes. The proposal is based on the conjecture that the inverse function, the logarithm, is not feasibly computable. We show that a proof of this conjecture would have important consequences for theoretical computer science, even under the assumption that $P \neq NP$.			

14.

KEY WORDS

cryptography
nondeterminism
polynomial time

LINK A

LINK B

LINK C

ROLE

WT

ROLE

WT

ROLE

WT